EXHIBIT 1

PREMISES COMPUTER SEARCH WARRANT AFFIDAVIT

THIS DRAFT IS CURRENT AS OF AUGUST 2014. GET THE MOST CURRENT VERSION OF THIS GO-BY FROM CCIPS ONLINE:

http://dojnet.doj.gov/criminal/ccips/warrants.htm

For help with any issues involving ECPA or computer searches, call the Computer Crime and Intellectual Property Section ("CCIPS"), Criminal Division, United States Department of Justice, at (202) 514-1026.

USAGE NOTES:

- This form should be used whenever a warrant is sought to allow agents to enter a premises and remove computers or storage media from the premises. A different form, "Electronic Device Search Warrant," should be used if you already have a laptop, cell phone, or similar device in your possession and want a warrant to examine it.
- Broad warrants that authorize the seizure of, for example, "any and all data" or "any and all computers," will often face particularity or over-breadth challenges. Use language of that type only when you have probable cause to believe any computer on the premises is contraband or an instrumentality.
- Premises search warrants generally "should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party." 28 C.F.R. § 59.4(a)(1). Any use of a search warrant for such a purpose should be done only in accordance with that regulation.
- Carefully review every sentence in your final affidavit to be certain that it is true in your case.
- For more information about searching and seizing computers with warrants, see Chapter 2 of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," available on CCIPS Online and http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009 .

PREMISES COMPUTER SEARCH WARRANT AFFIDAVIT

THIS DRAFT IS CURRENT AS OF AUGUST 2014. GET THE MOST CURRENT VERSION OF THIS GO-BY FROM CCIPS ONLINE:

http://dojnet.doj.gov/criminal/ccips/warrants.htm

For help with any issues involving ECPA or computer searches, call the Computer Crime and Intellectual Property Section ("CCIPS"), Criminal Division, United States Department of Justice, at (202) 514-1026.

USAGE NOTES:

- This form should be used whenever a warrant is sought to allow agents to enter a premises and remove computers or storage media from the premises. A different form, "Electronic Device Search Warrant," should be used if you already have a laptop, cell phone, or similar device in your possession and want a warrant to examine it.
- Broad warrants that authorize the seizure of, for example, "any and all data" or "any and all computers," will often face particularity or over-breadth challenges. Use language of that type only when you have probable cause to believe any computer on the premises is contraband or an instrumentality.
- Premises search warrants generally "should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party." 28 C.F.R. § 59.4(a)(1). Any use of a search warrant for such a purpose should be done only in accordance with that regulation.
- Carefully review every sentence in your final affidavit to be certain that it is true in your case.
- For more information about searching and seizing computers with warrants, see Chapter 2 of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," available on CCIPS Online and http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009 .

IN THE UNITED STATES DISTRICT COURT
FOR _____

IN THE MATTER OF THE SEARCH OF:
[[PREMISES ADDRESS]]

Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **[[AGENT NAME]]**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **[[PREMISES ADDRESS]]**, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a **[[TITLE]]** with the **[[AGENCY]]**, and have been since **[[DATE]]**. **[[DESCRIBE TRAINING AND EXPERIENCE INCLUDING EXPERTISE WITH COMPUTERS]].**

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. **[[IF APPROPRIATE, IDENTIFY PAST EFFORTS TO OBTAIN THE INFORMATION SOUGHT IN THIS WARRANT THROUGH OTHER SUBPOENAS OR**

WARRANTS IN THIS CASE. RELATE ANY COMMUNICATIONS WITH THE TARGET OF THE PROCESS. STATE WHETHER THE TARGET PROMISED TO PRESERVE THE EVIDENCE. ERR ON THE SIDE OF DISCLOSURE. EXAMPLE: I know that on August 26, 2009, a grand jury subpoena was sent to John Doe, owner of the PREMISES, requesting financial records. John Doe has not complied with that subpoena. John Doe has not moved to quash the subpoena. Efforts to communicate with John Doe regarding the subpoena have proven unsuccessful. The warrant I apply for today would allow seizure of the information called for by that subpoena, among other things. **]]**

PROBABLE CAUSE

5. [[establish probable cause to believe that evidence, fruits, or contraband can be found on each computer or storage medium that will be searched / seized, or to believe that the computers may be seized as contraband or instrumentalities.]]

TECHNICAL TERMS

6. **[[THIS SECTION MIGHT BE UNNECESSARY; DEFINE ONLY TECHNICAL TERMS AS NECESSARY TO SUPPORT PROBABLE CAUSE]]** Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

7. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

8. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. **[[FOR BUSINESS SEARCH CASES]]** Based on actual inspection of other evidence related to this investigation, [[spreadsheets, financial records, invoices]], I am aware that computer equipment was used to generate, store, and print documents used in the [[tax evasion, money laundering, drug trafficking, etc.]] scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

9. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and

malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic

and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. **[[FOR HACKING OR OTHER CASES WHERE A COMPUTER IS USED AS AN INSTRUMENTALITY TO COMMIT THE CRIME]]** I know that when an individual uses a computer to **[[**obtain unauthorized access to a victim computer over the Internet**]]**, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

10. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

11. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

12. **[[FOR CASES WHERE A RESIDENCE SHARED WITH OTHERS IS SEARCHED]]** Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

13. **[[INCLUDE THE FOLLOWING IF THERE IS A CONCERN ABOUT THE SEARCH UNREASONABLY IMPAIRING AN OPERATIONAL, OTHERWISE LEGAL BUSINESS]]** _____ ("the Company") is a functioning company that conducts legitimate business. The seizure of the Company's computers may limit the Company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

[[FORFEITURE]]

14. **[[USE THIS ONLY WHEN YOU ARE INVESTIGATING THE VIOLATION OF A STATUTE THAT ALLOWS FOR THE FORFEITURE OF FACILITATING PROPERTY OR CONTRABAND, AND YOU HAVE PROBABLE CAUSE TO BELIEVE THAT THE COMPUTER YOU ARE SEIZING WILL BE FORFEITABLE]]** This application requests the issuance of a warrant under 21 U.S.C. § 853(f) authorizing the seizure of property subject to forfeiture. This is appropriate because: (1) there is

probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, and (2) an order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture. There is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture, because **[[CONSULT THE ASSET FORFEITURE & MONEY LAUNDERING SECTION'S "FORFEITURE IN A BOX" PUBLICATION AVAILABLE AT http://dojnet.doj.gov/criminal/afoml/ FOR THE FORFEITURE STATUTE SPECIFIC TO YOUR CASE. EXAMPLE FOR A HACKING CASE FOLLOWS]]** 18 U.S.C. § 1030(i)(1)(A) provides that the defendant's "interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation" shall be forfeited to the United States.

CONCLUSION

15. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

16. **[[IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have**

learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]]

Respectfully submitted,

_____

[AGENT NAME]
Special Agent
[AGENCY]

Subscribed and sworn to before me
on June 13, 2016:

_____

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is **[[PREMISES ADDRESS]]**, further described as [[a red brick house]].

ATTACHMENT B

Property to be seized

1. All records relating to violations of **[[STATUTES]]**, those violations involving **[[SUSPECT]]** and occurring after **[[DATE]]**, including:

   a. **[[LIST SPECIFIC, PARTICULARIZED CATEGORIES OF INFORMATION HERE, EACH SUPPORTED BY FACTS IN YOUR PROBABLE CAUSE NARRATIVE SHOWING THAT THE INFORMATION IS EVIDENCE OF A CRIME OR IS CONTRABAND; EXAMPLES FOLLOW]]**

   b. Records and information relating to a conspiracy to defraud [[VICTIMS]];

   c. Records and information relating to an access of [[VICTIM COMPUTER]];

   d. Records and information relating to [[VICTIM COMPANY]];

   e. Records and information relating to the e-mail account [[ACCOUNT]];

   f. Records and information relating to the operation of a botnet;

   g. Records and information relating to the identity or location of the suspects;

   h. Records and information relating to communications with Internet Protocol addresses 149.101.1.114, 149.101.1.115, or 149.101.1.116;

   i. Records and information relating to malicious software;

j. Records and information relating to **[ADD SPECIFIC ITEMS IF NECESSARY]**.

2. [[IF OFFENSE INVOLVED COMPUTER AS FACILITATING PROPERTY, AN INSTRUMENTALITY, OR CONTAINER FOR CONTRABAND]] Computers or storage media used as a means to commit the violations described above, including **[[**downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).**]]**

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. **[[IF CASE INVOLVED THE INTERNET]]** Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.